552,586

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 November 2004 (04.11.2004)

PCT

(10) International Publication Number
WO 2004/095771 A1

(51) International Patent Classification[7]: H04L 9/30

(21) International Application Number:
PCT/JP2004/005528

(22) International Filing Date: 14 April 2004 (14.04.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2003-119973 24 April 2003 (24.04.2003) JP

(71) Applicant *(for all designated States except US)*: MATSUSHITA ELECTRIC INDUSTRIAL CO. LTD. [JP/JP]; 1006, Oaza Kadoma, Kadoma-shi, Osaka, 5718501 (JP).

(71) Applicant *(for US only)*: YAMAMICHI, Masami (heir of the deceased inventor).

(72) Inventor: YAMAMICHI, Masato (deceased).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: FUTA, Yuichi. OHMORI, Motoji. TATEBAYASHI, Makoto.

(74) Agent: NII, Hiromori; c/o NII Patent Firm, 3rd Floor, Shin-Osaka Suehiro Center Bldg., 11-26, Nishinakajima 3-chome, Yodogawa-ku, Osaka-shi,Osaka 5320011 (JP).

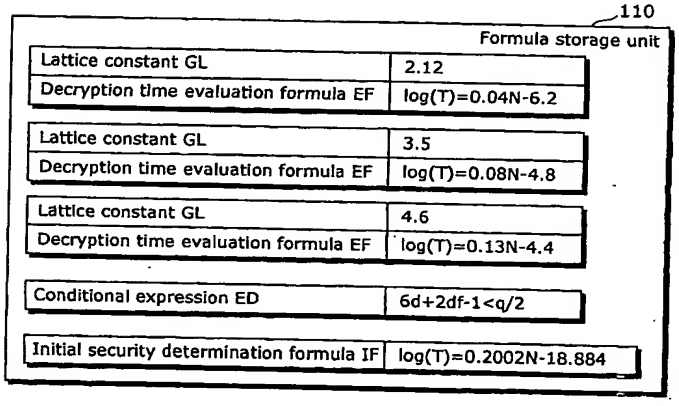
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: PARAMETER GENERATION APPARATUS, ENCRYPTION SYSTEM, DECRYPTION SYSTEM, ENCRYPTION APPARATUS, DECRYPTION APPARATUS, ENCRYPTION METHOD, DECRYPTION METHOD, AND PROGRAM THEREOF



(57) Abstract: A parameter generation apparatus for generating parameters causing no decryption error for an NTRU cryptosystem so that an encrypted communication can be carried out between an encryption apparatus and a decryption apparatus in a secure and reliable manner, is comprised of: a provisional parameter generation unit operable to generate a set of provisional parameters that do not cause any decryption errors, based on error condition information that is provided in advance, said error condition information indicating a condition for causing no decryption error; and an output parameter generation unit operable to generate an output parameter that does not cause any decryption errors, using said set of provisional parameters, based on a lattice constant that is calculated from said set of provisional parameters.

WO 2004/095771 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.